HIPAA Security Approach

(Example from HIPAAlive e-mail)

STEP 1 - AUDIT AND ASSESSMENT

Determine current security practices through analysis of current policies, Procedures and IS technologies. This includes actual practices as they relate to day to day operations and includes the following areas.

Components of Initial Audit & Assessment

- Local and wide area networks security
- Data communications dial-up access
- Workstation access and controls
- Disaster recovery plan
- Audit procedures
- Current technical mechanisms
- IS security policy/procedures
- Internet/intranet access
- Physical access controls
- HR policy and procedures
- Data storage and disposal
- Security training and awareness
- Current risk assessment
- User security policy/procedures

STEP 2 - MANAGEMENT REVIEW

Review the complete findings of the Audit and Risk Assessment with senior management, detail areas in need of remediation and determine priorities of remediation and implementation. Identify corporate goals and develop a project plan designed to attain those goals in an efficient and timely manner.

STEP 3 - DEVELOPMENT OF CORPORATE SECURITY STRATEGY

Design strategy to build security into the day to day business practices of the organization. This includes the policies and procedures necessary to integrate controls of complex, cross functional departments such as IS, HR, Facility Management, Clinical Operations, Patient Care, Pharmacy, Billing Operations and Administrative Operations.

Components of an Integrated Corporate Security Strategy - partial list

- Creating and updating policies
- Operating system controls
- Program change controls
- Disaster recovery planning
- Virus checking

- Disposal of information
- Single (Reduced) sign-on
- Employee education/awareness
- Asset and resource protection
- Documenting security standards
- Intrusion detection
- Network security/remote access
- Firewalls, encryption, active audit
- Termination procedures
- Unique user identification
- Web security
- Establish security committee

STEP 4 -REMEDIATION/IMPLEMENTATION

Implementation consists of a project management team that works with senior management and staff to develop and implement the specific remediation appropriate for the organization and consistent with senior management business goals.

Policy Development

- Release of medical information
- Medical staff bylaws and procedures
- Alias policy
- Network access
- Deactivation of user id's
- Remote access
- Internet usage/e-mail
- Paper disposal-media controls
- AIDS and AIDS related conditions, etc.
- Physical access
- Employee education/awareness training
- Disciplinary action
- Departmental/operating system
- Non-employee access
- Intrusion detection
- Electronic signature
- Distribution of sign-on id's/passwords
- Software distribution - copying policy
- Disaster recovery planning
- Patient information access

Technology Implementation Access Controls - Designed to conform to corporate policy and direction, ranging from simple user id/password to role based definition, directory/file access, biometrics (fingerprint, retina, etc.) single sign on and others. All technology is implemented to ensure that people and systems have necessary access and utilize resources as they are authorized and intended to be utilized.

Audit Controls - Provide controls, logs and regular reviews of how patient information is accessed and by whom. Audits must be at regular intervals and their findings must be documented.

Physical Access - Area/environmental definition with installation of control mechanisms such as card entry systems and combination locks. All physical access controls are designed in conformance with corporate policies developed to ensure that personnel have physical access to those areas of legitimate need, while preventing access to those without need.

Internet/Intranet - Firewalls, encryption, digital certificates and other Access mechanisms configured to support corporate policies. Ensures that risk, access and delivery of Internet/Intranet content conform to senior management business directives.

Intrusion Detection and On-Going Threat Analysis - Deployment of technology To ensure that attempts to circumvent security mechanisms are detected and to uncover any weaknesses prior to their exploitation. Provides continuing levels of risk, threat analysis and countermeasures.

STEP 5 - PERIODIC FOLLOW-UP AUDIT & ASSESSMENT

Follow-up audit and assessments are needed on a consistent basis to ensure that the Corporate Security Strategy is updated to accommodate changes in business process, industry standards and governmental regulations. This step ensures employee compliance to critical policies and procedures, provides a resource for on-going employee awareness training and provides methodology to accommodate technology changes. It also provides a continuing platform for maintenance and adjustment of policies and procedures to ensure practical conformance to business needs.